RECEIVED
CENTRAL FAX CENTER
JUN 12 2006

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission: 18

Application Number	10/044432
Filing Date	01/11/2002
First Named Inventor	Almalde
Art Unit	2136
Examiner Name	Corvelli
Attorney Docket Number	RPS9 2001 0091 US1

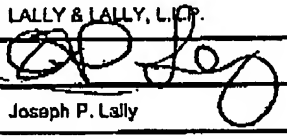
ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☑ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please identify below):

Remarks

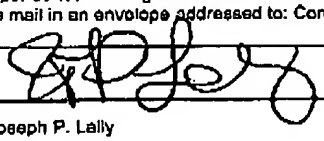
APPEAL BRIEF

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	LALLY & LALLY, L.L.P.		
Signature			
Printed name	Joseph P. Lally		
Date	June 12, 2006	Reg. No.	38,947

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name	Joseph P. Lally	Date	June 12, 2006

RECEIVED
CENTRAL FAX CENTER
JUN 12 2006

IBM.5255R PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	**Almeida**	§	Art Unit:	**2136**
Serial No.:	**10/044432**	§	Examiner:	**Cervetti**
Filed:	**January 11, 2002**	§	Attorney Docket:	**RPS9 2001 0091 US1**
For:	**Method and System for Programming a Non-Volatile Device in a Data Processing System**	§		

I, the undersigned Joseph P. Lally, hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the US Postal Service with sufficient postage as first class mail in an envelope addressed to: MAIL STOP AMENDMENT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

June 12, 2006
Date

Signature

APPEAL BRIEF

MAIL STOP APPEAL BRIEF
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

This paper is submitted pursuant to 37 CFR §41.37 in furtherance of the Notice of Appeal filed on April 12, 2006, following a Final Office Action dated August 12, 2005, to appeal final rejections of claims in the above referenced patent application to the Board of Patent Appeals and Interferences ("Board").

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The above referenced application is wholly assigned to International Business Machines Corporation ("IBM"), A New York corporation having a principle place of business at Armonk, New York.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals nor interferences known to Appellant which will directly affect, be directly affected by, or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

Claims 1-24 are pending in this application. Claims 1-24 stand rejected under the Final Office Action. More particularly:

Claims 1-2, 4-5, 9-10, 12-13, 17-18, and 20-21 stand rejected under 35 USC § 102(b) as being anticipated by Bright *et al.* (U.S. Patent No. 6,141,756), hereinafter "Bright".

Claims 3, 11, and 19 stand rejected under 35 USC § 103(a) as being unpatentable over Bright in view of Hughes (U.S. Patent No. 5,968,174), hereinafter "Hughes".

Claims 6-7, 14-15, and 22-23 stand rejected under 35 USC § 103(a) as being unpatentable over Bright in view of Cuccia *et al.* (U.S. Patent No. 6,151,676), hereinafter "Cuccia".

Claims 8, 16, and 24 also stand rejected under 35 USC § 103(a) as being unpatentable over Bright, and further in view of Cuccia. Appellant lists the rejection of these three claims separately from the rejection of claim 6-7, 14-15, and 22-23 despite the common references to maintain consistency with the form in which the Office Action identifies the grounds of rejection.

IV. STATUS OF AMENDMENTS

No amendments have been filed subsequent to the final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 recites computer executable instructions (computer code means), stored on a computer readable medium for programming a non-volatile storage element (105) of a data processing system (100) (see page 5, lines 1-4). The claim includes instructions for encrypting (304) a digital signature using a first encryption key [page 8, lines 8-9] and passing the encrypted signature (203) to a kernel routine (210) [page 8, lines 9-11]. Upon successfully decrypting (308) the signature (203), the kernel routine (210) transitions (311) system (100) to a real-mode state before calling a real mode flashing routine (204) to flash program (312) the non-volatile storage element (105) [page 6, lines 3-20], [page 8, lines 8-18].

Independent claim 9 recites a data processing system (100) including at least one processor (102), memory (106), and input means connected to a common bus (104, 110), [page 3, line 30 through page 4, line 19]. The system memory (106) contains at least a portion of a sequence of computer executable instructions for programming a non-volatile storage element (105) of the system (100). The instructions parallel the instructions recited in claim 1. Specifically, instructions for encrypting (304) a digital signature using a first encryption key [page 8, lines 8-9] and passing the encrypted signature (203) to a kernel routine (210) [page 8, lines 9-11]. Upon successfully decrypting (308) the signature (203), the kernel routine (210) transitions (311) system (100) to a real-mode state before calling a real mode flashing routine (204) to flash program (312) the non-volatile storage element (105) [page 6, lines 3-20], [page 8, lines 8-18].

Independent claim 17 recited a method (300) for programming a non-volatile storage element (105) in a data processing system. The method includes elements that parallel the code elements of independent claim 1. Specifically, the method (300) includes encrypting (304) a digital signature using a first encryption key [page 8, lines 8-9] and passing the encrypted signature (203) to a kernel routine (210) [page 8, lines 9-11]. Upon successfully decrypting (308) the signature (203), the kernel routine (210) transitions (311) system (100) to a real-mode state before calling a real mode flashing routine (204) to flash program (312) the non-volatile storage element (105) [page 6, lines 3-20], [page 8, lines 8-18].

Claims 1-16 all recite "computer code means", stored on a computer readable medium, for encrypting, passing, transitioning, programming, and so forth. Appellant is cognizant of the requirement under 37 CFR 41.37(c)(1)(v) to identify every means plus function and step plus function and to set forth the structure, material, or acts described in the specification as corresponding to each claimed function. To the extent the requirement is applicable to Beauregard claims, Appellant identify and set forth as follows:

Claim 1, computer code means for encrypting a digital signature using a first encryption key. For the acts described in the specification as corresponding to this element, see 304 of FIG 3 and accompanying text at page 8, lines 8-9.

Claim 1, computer code means for passing the encrypted signature to a kernel routine. For the acts described in the specification as corresponding to this element, text at page 8, lines 9-11.

Claim 1, computer code means, responsive to successfully decrypting the encrypted signature using a second encryption key, for transitioning the data processing system from a protected-mode to a real-mode. For the acts described in the specification as corresponding to these elements, see elements 308, 310, and 311 of FIG 3 and accompanying text at page 8, lines 11-15.

Claim 1, real-mode computer code means for flash programming the non-volatile storage element. For the acts described in the specification as corresponding to this element, see element 312 of FIG 3 and accompanying text at page 8, lines 15-16.

Claim 9, computer code means for encrypting a digital signature using a first encryption key. For the acts described in the specification as corresponding to this element, see 304 of FIG 3 and accompanying text at page 8, lines 8-9.

Claim 9, computer code means for passing the encrypted signature to a kernel routine. For the acts described in the specification as corresponding to this element, text at page 8, lines 9-11.

Claim 9, computer code means, responsive to successfully decrypting the encrypted signature using a second encryption key, for transitioning the data processing system from a protected-mode to a real-mode. For the acts described in the specification as corresponding to these elements, see elements 308, 310, and 311 of FIG 3 and accompanying text at page 8, lines 11-15.

Claim 9, real-mode computer code means for flash programming the non-volatile storage element. For the acts described in the specification as corresponding to this element, see element 312 of FIG 3 and accompanying text at page 8, lines 15-16.

VI. GROUND OF REJECTION TO BE REVIEWED ON APPEAL

The questions presented on this Appeal are:

1. Are independent claims 1, 9, and 17 anticipated by Bright under 35 USC § 102(b)?

VII. ARGUMENT

Claims 1, 9, and 17

Independent claims 1, 9, and 17 stand rejected under 35 USC § 102(b) as anticipated by Bright. Appellant respectfully submits that the anticipation rejection of independent claims 1, 9, and 17 is improper because the cited reference does not disclose all of claim limitations. Bright does not disclose either expressly or inherently a method or computer code for transitioning a data processing system from a protected mode to a real mode in response to successfully decrypting an encrypted signature.

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." MPEP 2131 (citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)). Each of the independent claims contains an element reciting a transition of a data processing system from a protected mode to a real mode responsive to successfully decrypting a signature. The Office Action indicates that column 4 lines 14-32 of Bright disclose this limitation. The cited portion of the reference reads as follows:

> If the program was found to be encrypted at step 305, the program is then decrypted at step 307. In the preferred embodiment, the decryption step is performed by the decryption processing section 107 of the processor 101. The decryption process is tailored to the type of encryption that was used to encrypt the program in the external device 103. If, for example, asymmetric encryption key was used to encrypt the program in the external device 103, then the same key would be used to decrypt the program at step 307. Similarly, if a public encryption key system was utilized, the program was encrypted by a public key and placed in the external device 103, and the processor 101 uses a private key to decrypt the same message. The key 113 used for decryption is embedded inside the processor in the preferred embodiment. The key 113 may be stored in RAM, ROM, programmable non-volatile memory, fixed hardware, and so forth. The decryption step may also include processing a key into another key or another piece of information to be used to decrypt the program.

Appellant submits that the cited passage does not disclose either expressly or inherently anything regarding transitioning a system from a protected mode to a real mode. The terms "protected mode" and "real mode" are well known in the field of microprocessor based data processing systems to refer to two different operating modes- a protected mode in which multiple applications can coexist because access to resources such as system memory is restricted or

protected by the operating system and a real mode in which the (sole) executing application can access any portion of the system memory and other resources. This distinction is also explicitly described in the specification as filed. See, e.g., paragraph beginning on page 2, line 4.

Bright does not disclose a data processing system transitioning to real mode. The terms "real mode" and "protected mode" simply do not occur in Bright. Nor does the term "kernel" or "kernel routine," which is recited in the second element of the claims under consideration. Bright does not disclose these terms expressly or inherently because transitioning a system from protected mode to real mode germane to Bright's technique for downloading an encrypted program that requires Bright to transition its processor to real mode as part of the process.

Appellant presented these arguments to the Examiner in response to a non-final office action. To the Appellant's amazement, the Examiner maintained the anticipation rejection under the following reasoning: "Assuming arguendo that Bright...does not expressly teach transitioning from a mode to a mode, Examiner submits that it would have been obvious to one of ordinary skill in the art to modify Bright to transition from one mode to another." Thus, the Examiner maintains his anticipation rejection by arguing that the claim elements not taught by the reference would have been obvious.

Appellant is more than a little surprised by the Examiner's flagrant disregard for the boundaries of the rejections that he chooses to issue. The cornerstone of anticipation is the teaching of all claim elements in a single reference. "The identical invention must be shown in as complete detail as is contained in the ... claim." Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). When an examiner is confronted with a claim that contains an element that is not expressly or inherently disclosed in the reference upon which the examiner is relying, the examiner has three choices. The examiner can find a reference that does anticipate the claim, issue a Section 103(a) rejection, provided that the examiner can establish a prima facie showing of obviousness, or indicate the allowability of the claim. One thing that an Examiner is clearly not permitted to do is to maintain an anticipation rejection on grounds of obviousness.

Appellant recognizes the Examiner's not so subtle motivation. If examiners could issue Section 102 rejections based on partial anticipation, they could avoid the cumbersome task of establishing obviousness when they find themselves without an anticipating reference.

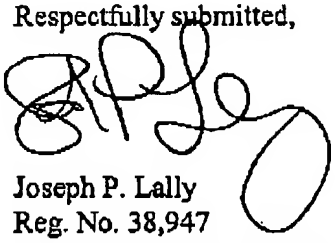
Fortunately for Appellant, however, the distinction between Section 102 and Section 103 is likely to survive the Examiner's hopefully temporary blindness.

Because the cited reference does not disclose either expressly or inherently a limitation found in the claims under consideration, the anticipation rejection is improper and Appellant respectfully requests the Board to reverse the rejection.

CONCLUSION

In view of the foregoing, Appellant submits that the anticipation rejections of independent claims 1, 9, and 17 are improper and Appellant respectfully requests the Board to reverse the rejection of these claims and remand the case to the Examiner with an order to allow the claims or issue a properly founded rejection.

Respectfully submitted,



Joseph P. Lally
Reg. No. 38,947
ATTORNEY FOR APPELLANT

LALLY & LALLY, LLP
P.O. Box 684749
Austin, Texas 78768-4749
512.428.9870
512.428.9871 (FAX)

JPL/mmm

VIII. CLAIMS APPENDIX

TEXT OF CLAIMS PRESENTED ON APPEAL

WHAT IS CLAIMED IS:

1 (original). A computer program product comprising processor executable instructions for programming a non-volatile storage element in a data processing system, the instructions being stored on a computer readable medium, comprising:

computer code means for encrypting a digital signature using a first encryption key;

computer code means for passing the encrypted signature to a kernel routine;

computer code means, responsive to successfully decrypting the encrypted signature using a second encryption key, for transitioning the data processing system from a protected-mode to a real-mode; and

real-mode computer code means for flash programming the non-volatile storage element.

2 (original). The computer program product of claim 1, wherein the code means for encrypting the digital signature is non-privileged code.

3 (original). The computer program product of claim 2, wherein the code means for passing the encrypted signature to the kernel routine comprises code means for executing a system call from the non-privileged code and passing the signature as a parameter of the system call.

4 (original). The computer program product of claim 1, wherein the first encryption key is a private key and the second encryption key is a public key, wherein the public key and private key are generated from a common algorithm.

5 (original). The computer program product of claim 1, further comprising code means for generating the digital signature, wherein the digital signature includes information that is indicative of the data processing system.

6 (original). The computer program product of claim 5, wherein the digital signature is generated based at least in part upon dynamic information.

7 (original). The computer program product of claim 6, wherein the digital signature is generated at least in part based further upon information including a corresponding hostname and process ID.

8 (original). The computer program product of claim 1, further comprising code means for generating a random number as the digital signature.

9 (original). A data processing system including at least one processor, memory, and input means connected to a common bus, wherein the system memory contains at least a portion of a sequence of computer executable instructions for programming a non-volatile storage element of the data processing system, the instructions comprising:

computer code means for encrypting a digital signature using a first encryption key;

computer code means for passing the encrypted signature to a kernel routine;

computer code means, responsive to successfully decrypting the encrypted signature using a second encryption key, for transitioning the data processing system from a protected-mode to a real-mode; and

real-mode computer code means for flash programming the non-volatile storage element.

10 (original). The data processing system of claim 9, wherein the code means for encrypting the digital signature is non-privileged code.

11 (original). The data processing system of claim 10, wherein the code means for passing the encrypted signature to the kernel routine comprises code means for executing a system call from the non-privileged code and passing the signature as a parameter of the system call.

12 (original). The data processing system of claim 9, wherein the first encryption key is a private key and the second encryption key is a public key, wherein the public key and private key are generated from a common algorithm.

13 (original). The data processing system of claim 9, further comprising code means for generating the digital signature, wherein the digital signature includes information that is indicative of the data processing system.

14 (original). The data processing system of claim 13, wherein the digital signature is generated based at least in part upon dynamic information.

15 (original). The data processing system of claim 14, wherein the digital signature is generated at least in part based further upon information including a corresponding hostname and process ID.

16 (original). The data processing system of claim 9, further comprising code means for generating a random number as the digital signature.

17 (original). A method of programming a non-volatile storage element in a data processing system, comprising:

encrypting a digital signature using a first encryption key;

passing the encrypted signature to a kernel code routine;

responsive to successfully decrypting the encrypted signature using a second encryption key, transitioning the data processing system from a protected-mode to a real-mode with the kernel code routine; and

flash programming the non-volatile storage element in real mode.

18 (original). The method of claim 17, wherein encrypting the digital signature comprises encrypting the digital signature with non-privileged code.

19 (original). The method of claim 18, wherein passing the encrypted signature to the kernel routine comprises executing a system call from the non-privileged code and passing the signature as a parameter of the system call.

20 (original). The method of claim 17, wherein the first encryption key is a private key and the second encryption key is a public key, wherein the public key and private key are generated from a common algorithm.

21 (original). The method of claim 17, further comprising generating the digital signature, wherein the digital signature includes information that is indicative of the data processing system.

22 (original). The method of claim 21, wherein the digital signature is generated based at least in part upon dynamic information.

23 (original). The method of claim 22, wherein the digital signature is generated at least in part based further upon information including a corresponding hostname and process ID.

24 (original). The method of claim 17, further comprising code means for generating a random number as the digital signature.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.